REMARKS

Applicant has studied the Office Action dated July 27, 2007 and has made amendments to the claims. It is submitted that the application, as amended, is in condition for allowance. Claims 1-20 are pending. Claims 1, 3-6, 8-17, and 20 have been amended. Reconsideration and allowance of the claims in view of the above amendments and the following remarks are respectfully requested.

The title of the invention was objected to as not being descriptive. The title has been amended to be more clearly indicative of the invention to which the claims are directed.

Claims 5, 8, 15, and 20 were objected to because of "informalities". Claims 5, 8, 15, and 20 have been amended in light of the specific comment of the Examiner. It is submitted that all of the pending claims fulfill the requirements of 35 U.S.C. § 112. Therefore, it is respectfully submitted that the objection to claims 5, 8, 15, and 20 should be withdrawn.

Claims 10-16 were rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. Applicant has amended claims 10-16 so that they recite a tangible computer readable medium encoded with a program for identifying spoofed emails, with the program comprising instructions for performing a method comprising the recited steps. Applicant respectfully submits that a computer readable medium encoded with a program containing instructions for performing recited steps complies with the written description requirement and is statutory subject matter. Therefore, it is respectfully submitted that the rejection of claims 10-16 under 35 U.S.C. § 112, first paragraph, should be withdrawn.

Claims 1-20 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The claims have been amended to remove the language that was objected to by the Examiner. Therefore, it is respectfully submitted that the rejection of claims 1-20 under 35 U.S.C. § 112, second paragraph, should be withdrawn.

Claims 1-20 were rejected under 35 U.S.C. § 102(e) as being anticipated by Bishop, JR., et al. (U.S. Patent Application Publication No. 2004/0148356). Claims 1-20 were also rejected under 35 U.S.C. § 102(a) as being anticipated by Goldman (U.S. Patent Application Publication No. 2003/0233418). Claims 1-20 were also rejected under 35 U.S.C. § 102(e) as being anticipated by Chang (U.S. Patent Application Publication No. 2004/0192691). These rejections are respectfully traversed.

The present invention is directed to an efficient and easy-to-implement method for identifying spoofed email. The present invention makes it extremely difficult, if not impossible, for a malicious sender outside of a network, company, Internet domain, intranet, or enterprise to pretend to be a user within that network, so as to make it less likely that a recipient will open harmful or spam email based on the apparent sender. This substantially prevents senders outside of a network from sending email to recipients within that network while falsely claiming that the email originated within the network. Such spoofed email is processed to indicate its external origin before it is received by the intended recipient.

The Bishop reference is directed toward an electronic messaging system for private messaging. Bishop teaches sending a message from a sender to a message server. The message server verifies the sender is a sending agent that is registered with the message server and decrypts a message header in the message. This decryption process allows the server to ascertain one or more recipients that are to receive the message. The messaging server also verifies whether the one or more recipients are recipient agents that are registered with the message server. The message is then sent from the message server to the one or more recipient agents that are registered with the message server.

The Goldman reference is directed toward managing data associated with incoming electronic messages including filtering incoming electronic messages according to the sender's address. Goldman also teaches a request/response technique for categorizing a sender's address as authorized, unauthorized, or unconfirmed, which categorizations are stored in an associated data structure. Goldman further teaches a number of complementary techniques for facilitating the process of populating the data structures that identify sender's addresses associated with authorized and

unauthorized senders. A filter module filters out unsolicited electronic messages. A categorization module categorizes sender's addresses associated with electronic messages according to a request/response protocol, which enables incoming electronic messages to be filtered and unwanted electronic messages discarded or rejected.

Chang is directed toward providing an open email directory. An email directory and forwarding service charges an email message sender a refundable sender's fee for each email message sent. The directory allows an email message recipient to be located in a search by other users or commercial senders using biographical and affinity information voluntarily provided by the recipient. Chang also teaches an internet identity registry and a sender verification service. For example, the internet identity registry allows verification of the identity of an email sender or recipient, or an internet user in general. The identity registry can also be searched by identity or affinity. Chang teaches that by combining a fee-based email forwarding service with a searchable directory of verified senders and recipients, Chang achieves anti-spam, social networking, question-answering, targeted advertising and direct marketing objectives simultaneously.

Nowhere does Bishop, Goldman, or Chang teach determining whether a sender address associated with a received email is associated with a mailbox within the same network as the receiver. Also, nowhere does Chang, Goldman, or Chang teach modifying the sender address to indicate that the email purporting to be from the same network as the recipient was actually sent from a mailbox external to the network, and then sending the email with the modified sender address to the recipient. Bishop, Goldman, and Chang are completely silent on at least these elements.

Independent claims 1, 10, and 17 have been amended to more clearly recite the present invention. In particular, independent claim 1 (and similarly independent claims 10 and 17) has been amended to recite:

> *receiving an email addressed to a recipient in a first network, the email including a plurality of headers, wherein at least one of the plurality of headers includes a sender address;*
>
> *determining whether the sender address indicates a mailbox from within the first network;*
>
> *when the sender address indicates a mailbox from within the first network, modifying at least a portion of the sender address so as to produce a modified sender*

address that indicates to the recipient that the email is associated with a mailbox that is external to the first network; and

sending the email with the modified sender address to the recipient, the modified sender address being visible to the recipient.

With respect to the modifying and sending steps, the Examiner directs the Applicant to col. 22 of Bishop; col. 6 of Goldman; and col. 5 of Chang. Col. 22 (and the remaining columns) of Bishop is completely silent on modifying the sender address. Bishop is directed at using encryption and digital signatures for verifying a user. For example, col. 22, paragraphs [0228]-[0232] teach:

> The final goal of the present invention, that of spam prevention, is accomplished not with additional distributed processing, but via careful operation of the procedures and elements of Private Messaging System 100....Beginning with System Perspective 2200, the first step is to establish a message privacy service using Private Messaging System 100 at step 2201, preferably by deploying an instance of Trusted Courier 120 and Inviting and Registering users. As has been discussed previously, essential to ensuring the authenticity of users is the practice, noted in step 2202, of verifying the messaging address for each prospective new user of the system using the Invitation and Registration processes described above. Then at step 2203, the system will authenticate the sender of every message against this verified registration, thereby preventing spoofing altogether.
>
> To ensure that no one floods the system automatically with far more messages than real user can compose and send, at step 2204 the system is operated in such a manner as to limit the number of Private and Restricted messages each user may send in a particular period. This governor will tend to prevent the typical sender of bulk commercial messages from using the service because it will permit too few messages for an effective marketing campaign. In step 2205 a fair price is charged to each user, according to the value of the service for individuals who require Private or Restricted messages. Again, this price will generally be higher than a spammer can afford to pay for the limited number of messages. Finally, in step 2206 the system is operated in such a manner as to attract as many users as possible, with the ultimate goal of serving every legitimate user in the network at large. Every user served in the Private Messaging System 100 is a user to whom spam is not delivered, so the more users the system has, the smaller will be spammers' audience.
>
> From the User's Perspective 2210, spam prevention begins at step 2211 with the decision and action to register for the services of Private Messaging System 100. In step 2212, the user will provide an authentic messaging address that is proven using the Registration process. This assures this user and all others that every user in the system is real. Step 2213 depicts the user exchanging Private and Restricted messages with other users, building not only confidence in the system and its services but also a set of correspondents who also use the system. When a critical mass of correspondents are present in the system, at step 2214 the user may choose to ignore all messages that do not arrive via the Private Messaging System 100. A (*Sic*) this point, the user becomes invulnerable to spam.

> Finally, from a Spammer's Perspective 2220 there are two possible approaches to Private Messaging System 100. First, the spammer may wish to join the system as a user but continue exercising current common practices such as header forgery. Step 2221 prevents this by requiring each user to have a messaging address that can be verified by the Invitation and Registration processes. Such a spammer will fail to register at step 2222. As stated in step 2223, the spoofing spammer will therefore be unable to send Private or Restricted messages to anyone. Since, as stated in step 2224 all legitimate users will by now be ignoring every message that does not arrive via this system, the spammer's potential audience is significantly reduced.

Furthermore, Bishop teaches that a sender must register with the Private messaging system. Bishop teaches at paragraph [0083] that "[the invitation process, by sending a message to the invited address, ensures that a registering user can in fact receive messages at the claimed address. This prevents fraudulent attempts to register another person's messaging address and thereby impersonate that individual." Bishop also teaches at paragraph [0094] that cryptographic keys are created for signing messages to be sent and decrypting received messages. Bishop goes on to teach at paragraphs [0103]-[0104] that when a message is received from a sender, the sender's address is used to retrieve an account entry from a user database. The two digital signatures in the message are validated, and if either of them fails the message is discarded.

Bishop is completely silent on modifying the sender address when the sender address indicates a mailbox from within the first network. Bishop clearly does not teach modifying a sender address. Applicant has amended claim 1 to more clearly recite that "when the sender address indicates a mailbox from within the first network, modifying at least a portion of the sender address so as to produce a modified sender address that indicates to the recipient that the email is associated with a mailbox that is external to the first network." Bishop clearly does not teach such a feature.

Bishop is also silent on sending the email with the modified sender address to the sender. As explained above, Bishop deletes a message from a sender when a message's signatures fail to be validated. The present invention recites "sending the email with the modified sender address to the recipient, the modified sender address being visible to the recipient." Bishop is completely silent on modifying a sender address and modifying the sender address in a way that is visible to a recipient when a recipient receives the email.

One advantage of the present invention is that the sender address is modified so that a recipient is notified that even though the email purports to originate from his/her network, the email actually originated outside of the network. For example, a recipient can be a part of Network_A and have an email address of recipient1@Network_A.com. A spoof email may originate from Network_Z but may have the appearance of sender@Network_A.com. The whole idea behind a spoof email is to appear as having been sent from a particular network when the email was actually sent from another network. Therefore, when the present invention detects that an email is purporting to be from the same network as the recipient when it was not sent from that network, the sender address associated with the email is modified to notify the sender that the email was sent from a mailbox external to his/her network. Figures 2 and 4 of the Specification as originally filed show an example of an original sender address and a modified address. Continuing with the current example, the present invention modifies the original sender address of sender@Network_A.com to sender@externalto.Network_A.com. This indicates to a recipient that the email was sent from a mailbox external to his/her network. (This is only one example illustrating a modified email address and is not meant to limit the present invention.) Nowhere does Bishop teach such a feature. Accordingly, the presently claimed invention distinguishes over Bishop for at least these reasons.

With respect to Goldman, Goldman teaches filtering messages from a sender based on a sender's address being classified as authorized, unauthorized, or confirmed. These classifications can be assigned to a sender's address based on responses to questions and whether the responses are received within a given amount of time. Col. 6, where the Examiner directs Applicant, merely states that a message can be sent to a manager of a domain associated with the sender's address so that the manager can verify whether the sender is a legitimate. Col. 6 also goes on to teach how to classify a sender's address based on a sender sending a response to a request for a response.

Goldman is completely silent on modifying a sender address and clearly does not teach the amended elements of:

> *when the sender address indicates a mailbox from within the first network, modifying at least a portion of the sender address so as to produce a modified sender address that indicates to the recipient that the email is associated with a mailbox that is external to the first network; and*
>
> *sending the email with the modified sender address to the recipient, the*

modified sender address being visible to the recipient.

Accordingly, the present invention distinguishes over Goldman for at least these reasons.

With respect to Chang, Chang is directed towards a fee based email system for reducing spam and a registry of verified senders. When an email is received the registry can be queried to determine if the sender is verified. Col. 5, where the Examiner directs Applicant to, is completely silent on the claim elements of:

> *when the sender address indicates a mailbox from within the first network, modifying at least a portion of the sender address so as to produce a modified sender address that indicates to the recipient that the email is associated with a mailbox that is external to the first network; and*
>
> *sending the email with the modified sender address to the recipient, the modified sender address being visible to the recipient.*

In fact, paragraph [0046] states:

> ...If the sender of an eMail message is not an existing member, an invitation-to-join or another appropriate notification message 804 may be sent to the sender. Any eMail message that is not delivered to private mailbox 802 (e.g., for a reason such as unverified sender, or insufficient sender's fee) may be placed in escrow with the service, left in the original public mailbox until the deficiency is corrected, or may be rejected immediately or after a specified time delay. If the sender is a member and the applicable sender's fee requested is within the sender's specified allowable limits (both for the eMail message and the sender's specified daily or weekly total, for example), the sender's fee is deducted from the sender's account, and the eMail message is forwarded to the recipient's private mailbox. Otherwise, i.e., if the sender authorization is non-conforming or deficient, a fee authorization request is sent to the sender. Requesting authorization from the sender when the eMail request is non-conforming, provides a method to catch a "spoofed" sender address (i.e., an email addressed fabricated by a spammer imposter to hide its true identity) and to prevent significant damage. If instructed by the member, the eMail service can forward unverified eMail messages to a separate mailbox set aside for probable spam.

As can be seen, Chang does not teach modifying a sender address to indicate to a recipient that an email is a spoof email. Chang uses a fee-based system and a verified sender registry to determine if an email address has been fabricated. Nowhere does Chang teach modifying a sender address

Chang is completely silent on modifying a sender address and clearly does not teach the

recited modifying and sending steps. Accordingly, the present invention distinguishes over Chang for at least these reasons.

Claims 2-9, 11-16, and 18-20 depend from claims 1, 10, and 17 respectfully, and since dependent claims include all the limitations of their independent claim, claims 2-9, 11-16, and 18-20 are also allowable. Additionally, Applicant gives additional arguments with respect to claims 6-9 below.

Claims 6-8 are directed toward modifying the sender address. The Examiner cites col. 7 of Bishop, col. 6 and col. 9 of Goldman, and col. 5 of Chang in support of rejecting these claims. However, each of these citations are completely silent on modifying a sender address, especially on "appending a predetermined sub-domain to the sender address" and modifying at least one of a domain and a sub-domain of the sender address. The citations given by the Examiner do not even mention modifying the sender address. Accordingly, claims 6-8 also distinguish over Bishop, Goldman, and Chang for at least these reasons as well.

With respect to claim 9, the Examiner cites col. 18 of Bishop, col. 6 of Goldman, and cols. 6-7 of Chang in support of rejecting this claim. Claim 9 recites:

> *receiving a second email, the second email being from the recipient and being addressed to the modified sender address;*
>
> *modifying the modified sender address so as to produce the sender address; and*
>
> *sending the second email with the sender address.*

Nowhere does Bishop, Goldman, or Chang, teach changing the modified sender address back to the sender address received from the sender when the recipient replies to the email message with the modified sender address. The citations given by the Examiner are completely silent on this claim element. Using the above example, nowhere does Bishop, Goldman, or Chang teach receiving a reply email from a recipient with a sender address of sender@externalto.Network_A.com and changing back the sender address to sender@Network_A.com prior to sending out the reply email to the sender. Accordingly, claim 9 also distinguishes over Bishop, Goldman, and Chang for at least this reason as well.

In view of the foregoing, it is respectfully submitted that the application and the claims are in condition for allowance. Reexamination and reconsideration of the application, as amended, are requested.

No amendment made was related to the statutory requirements of patentability unless expressly stated herein. No amendment made was for the purpose of narrowing the scope of any claim, unless Applicant has argued herein that such amendment was made to distinguish over a particular reference or combination of references.

If for any reason the Examiner finds the application other than in condition for allowance, the Examiner is invited to call the undersigned attorney at (561) 989-9811 should the Examiner believe a telephone interview would advance the prosecution of the application.

Respectfully submitted,

Date: December 27, 2007

By: /Stephen Bongini/
Stephen Bongini
Reg. No. 40,917
Attorney for Applicant

FLEIT KAIN GIBBONS
GUTMAN BONGINI & BIANCO P.L.
One Boca Commerce Center
551 Northwest 77th Street, Suite 111
Boca Raton, Florida 33487
Telephone: (561) 989-9811
Facsimile: (561) 989-9812